Exploring some topologies of coupled chaotic networks

Oleg Garasym, René Lozi, Ina Taralova

Exploring some topologies of coupled chaotic networks

Oleg Garasym [1], René Lozi [2], Ina Taralova [1],
[1] Ecole Centrale de Nantes, France Email: oleg.garasym, ina.taralova@irccyn.ec-nantes.fr
[2] Laboratoire J. A. Dieudonné, UMR CNRS 7351 Nice Sophia-Antipolis, NICE Email: rlozi@unice.fr

***Abstract*—This paper is devoted to the design of new chaotic Pseudo Random Number Generator (CPRNG). Exploring several topologies of network of 1-D coupled chaotic mapping, we focus first on two dimensional networks. Two topologically coupled maps are studied: TTL^{RC} non-alternate, and TTL^{SC} alternate. The primary idea of the novel maps has been based on an original coupling of the tent and logistic maps to achieve excellent random properties and homogeneous /uniform/ density in the phase plane, thus guaranteeing maximum security when used for chaos base cryptography. In this aim two new nonlinear CPRNG: $MTTL_2^{SC}$ and $NTTL_2$ are proposed. The maps successfully passed numerous statistical, graphical and numerical tests, due to proposed ring coupling and injection mechanisms.**

***Index Terms*—Chaos, tent-logistic map, randomness.**

I. Introduction

THE tremendous development of new IT technologies, e-banking, e-purchasing, etc. nowadays increases incessantly the needs for new and more secure cryptosystems. The latter are used for information encryption, pushing forward the demand for more efficient and secure pseudo-random number generators [1]. At the same time, chaotic maps show up as perfect candidates able to generate independent and secure pseudo-random sequences (used as information carriers or directly involved in the process of encryption/decryption). However, the majority of well-known chaotic maps are not naturally suitable for encryption [2] and most of them don't exhibit even satisfactory properties for encryption. To deal with this open problem, we propose the unusual idea to couple tent and logistic map, and to add an injection mechanism to keep bounded the escaping orbits.

In 1973, sir Robert May, a famous biologist introduced the nonlinear, discrete time dynamical system called logistic equation:

$$x_{n+1} = rx_n(1 - x_n) \tag{1}$$

as a model for the fluctuations in the population of fruit flies in a closed container with constant food [3]. Since that early time this logistic equation has been extensively studied especially by May [4], and Mitchell Feigenbaum [5] under the equivalent form:

$$x_{n+1} = f_\mu(x_n) \tag{2}$$

where

$$f_\mu(x_n) \equiv L_\mu(x) = 1 - \mu x^2 \tag{3}$$

Another often studied discrete dynamical system is defined by the symmetric tent map:

$$f_\mu \equiv T_\mu = 1 - \mu|x| \tag{4}$$

In both cases, μ is a control parameter that has impact to chaotic degree, and those mappings are sending the one-dimensional interval $[-1, 1]$ into itself.

Those two maps have also been fully explored with the hope of generating pseudo-random numbers [6]. However the collapsing of iterates of dynamical systems or at least the existence of very short periodic orbits, their non constant invariant measure, and the easily recognized shape of the function in the phase space should lead to avoid the use of such one-dimensional map (logistic, baker, or tent, etc.) or two dimensional map (Hénon, standard or Belykh, etc.) as a pseudo-random number generator (see [7] for a survey). However, the very simple implementation in computer program of chaotic dynamical systems led some authors to use it as a base of cryptosystem [8]. They are topologically conjugate, that means they have similar topological properties (distribution, chaoticity, etc.) however due to the structure of number in computer realization their numerical behaviour differs drastically. Therefore the original idea here is to combine features of tent (T_μ) and logistic (L_μ) maps to achieve new map with improved properties, trough combination of several network topologies. In this paper we propose new ideas of tent and logistic maps coupling, based on the analogy between mathematical circuits and electrical circuits [9].

II. Exploring topologies of network of coupled chaotic maps

Ring and auto-coupling of chaotic maps (or circuits) enables to combine the individual circuit's dynamics, and therefore, to obtain more complex dynamic behaviour. For instance, different ways of coupling several Chua's circuits gives rise to hyperchaos [9]. It should be emphasized that these representations (Fig. 1) are also a perfect tool to investigate the topology of the map.

Looking at the equations we can inverse the shape of the graph of the tent map T on the step of logistic map L. Thus, our proposition has the form:

$$f_\mu(x) \equiv TL_\mu(x) = \mu|x| - \mu x^2 = \mu(|x| - x^2) \tag{5}$$

Recall that both logistic and tent maps have never been used in cryptography because they have weak security (collapsing

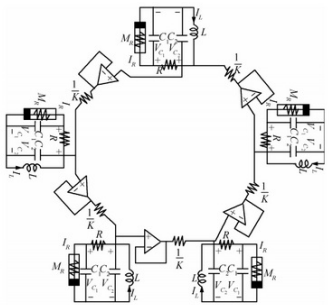


Fig. 1. Circuits of ultra-weak coupling of chaotic Chua's circuits

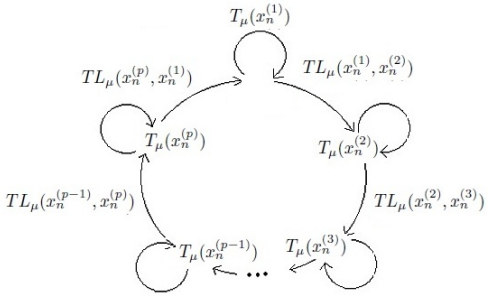


Fig. 2. Auto and ring-coupling between states of the M_p

effect) [10], [11] if applied alone. Thus, systems are often used in modified form to construct PRNG [12], [13]. The Lozi system [14] provides method to increase randomness properties of the tent map over its coupling. In another way, we propose to couple T_μ map over combination with TL_μ map (5). When used in more than one dimension, TL_μ map can be considered as a two dimensional map:

$$TL_\mu(x^{(1)}, x^{(2)}) = \mu(|x^{(1)}| - (x^{(2)})^2) \tag{6}$$

Hence it is possible to define a mapping M_p from $[-1,1]^p \to [-1,1]^p$

$$M_p \begin{pmatrix} x_n^{(1)} \\ x_n^{(2)} \\ \vdots \\ x_n^{(p)} \end{pmatrix} = \begin{pmatrix} x_{n+1}^{(1)} \\ x_{n+1}^{(2)} \\ \vdots \\ x_{n+1}^{(p)} \end{pmatrix} = \begin{cases} T_\mu(x_n^{(1)}) + TL_\mu(x_n^{(1)}, x_n^{(2)}) \\ T_\mu(x_n^{(2)}) + TL_\mu(x_n^{(2)}, x_n^{(3)}) \\ \vdots \\ T_\mu(x_n^{(p)}) + TL_\mu(x_n^{(p)}, x_n^{(1)}) \end{cases} \tag{7}$$

Note that the system dynamics is unstable and trajectories quickly spread out. Therefore, to solve the problem of holding dynamics in the bound $[-1,1]^p$ the following injection mechanism has to be used:

$$\begin{array}{c} \text{if } x_{n+1}^{(i)} < -1 \\ \text{then add } 2 \\ \text{if } x_{n+1}^{(i)} > 1 \\ \text{then substract } 2 \end{array} \tag{8}$$

in this case for $1 \le i \le p$, points come back from $[-3,3]^p$ to $[-1,1]^p$.

Auto and ring-coupling between states (Fig.2) of the map and injection mechanism influence the system dynamics making its dynamics complex enough for our application purposes.

Used in conjunction with T_μ the TL_μ function allows to establish mutual influence between system states. The function is attractive because it performs contraction and stretching distance between states improving chaotic distribution. Thus, TL_μ function is a powerful tool to change dynamics.

The coupling of the simple states has excellent effect on chaos achieving, because:

- Simple states interact with global system dynamics, being a part of it.
- The states interaction has a global effect.

Hence, if we use TL_μ to make impact on the dynamics of simple maps, then excellent effect on chaoticity and randomness could be achieved. The proposed function improve the complexity of a simple map.

Note that the system (7) can be seen in the scope of a general point of view, introducing constants k^i which generalize considered topologies. It is called alternate if $k^i = +1$, $1 \le i \le p$, or non-alternate if $k^i = (-1)^i$, $1 \le i \le p$; or $k^i = -1$, $1 \le i \le p$. It can be a mix of alternate and non-alternate if $k^i = +1$ or -1 randomly. As well it has been already shown that the coupling could improve the performances of well known chaotic attractors (Chua, Lorenz, Rossler, etc.) for application purposes [9].

$$M_p \begin{pmatrix} x_n^{(1)} \\ x_n^{(2)} \\ \vdots \\ x_n^{(p)} \end{pmatrix} = \begin{pmatrix} x_{n+1}^{(1)} \\ x_{n+1}^{(2)} \\ \vdots \\ x_{n+1}^{(p)} \end{pmatrix} = \begin{cases} T_\mu(x_n^{(1)}) + k^1 \times TL_\mu(x_n^{(1)}, x_n^{(2)}) \\ T_\mu(x_n^{(2)}) + k^2 \times TL_\mu(x_n^{(2)}, x_n^{(3)}) \\ \vdots \\ T_\mu(x_n^{(p)}) + k^p \times TL_\mu(x_n^{(p)}, x_n^{(1)}) \end{cases} \tag{9}$$

In this paper we will discuss only systems exhibiting the best properties for CPRNG. Therefore, we will consider only two 2-D systems: $TTL_\mu^{RC}(x_n^{(2)}, x_n^{(1)})$ **non-alternate**:

$$TTL_\mu^{RC} : \begin{cases} x_{n+1}^{(1)} = 1 - \mu|x_n^{(1)}| + \mu(|x_n^{(2)}| - (x_n^{(1)})^2) \\ x_{n+1}^{(2)} = 1 - \mu|x_n^{(2)}| + \mu(|x_n^{(1)}| - (x_n^{(2)})^2) \end{cases} \tag{10}$$

and $TTL_\mu^{SC}(x_n^{(1)}, x_n^{(2)})$ **alternate**:

$$TTL_\mu^{SC} : \begin{cases} x_{n+1}^{(1)} = 1 - \mu|x_n^{(1)}| - \mu(|x_n^{(1)}| - (x_n^{(2)})^2) \\ x_{n+1}^{(2)} = 1 - \mu|x_n^{(2)}| + \mu(|x_n^{(1)}| - (x_n^{(2)})^2) \end{cases} \tag{11}$$

Here RC stand for ring-coupling and SC for standard coupling.

III. Randomness study of the new maps TTL_μ^{RC} and TTL_μ^{SC}

We are now assessing the randomness of both selected maps. The associated dynamical system is considered to be random and could be applied to cryptosystems if the chaotic generator meets the requirements 1-8 on Fig.3. If one of the criterion is not satisfied, the behavior is less random than expected.

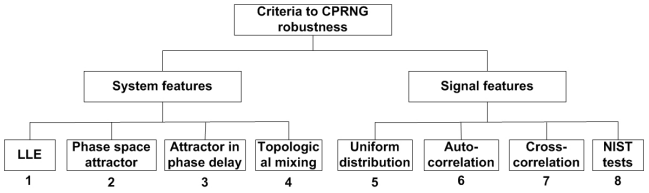
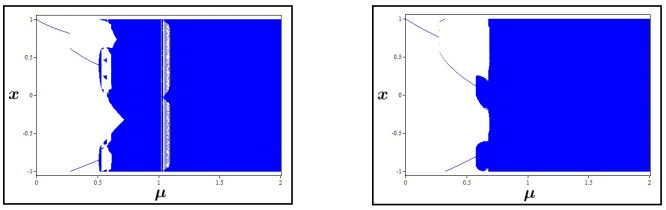


Fig. 3. The main criteria for PRNG robustness

As it has been summarized in the scheme (Fig.3) a generator could be taken into consideration for cryptography application if and only if each criterion is satisfied.

Chaotic map behavior primarily depends on the initial guess x_0 and "control" parameter μ. However, the dependence versus the initial guess, x_0 has less importance when the global phase portrait is scrutinized. Thus, to study the dependency of parameter μ a bifurcation diagram is an appropriate tool. To create the diagram for the new map, a particular initial value of x_0 is randomly selected, and the map is iterated for a given μ. A certain number of firstly generated points is cut off to remove the transient part of the iterated points, and the following points are plotted. Afterwards, the process is repeated incrementing slightly μ.

To plot the bifurcation diagram for the 2-D systems TTL_μ^{RC} non-alternate (Fig. 4.a) and TTL_μ^{SC} alternate (Fig. 4.b), 10,000 iterations have been generated for each initial value and the first 1,000 points have been cut off as transient. Thus, 9,000 points are plotted for each μ parameter. The graphs are the same for $x^{(1)}$ and $x^{(2)}$.



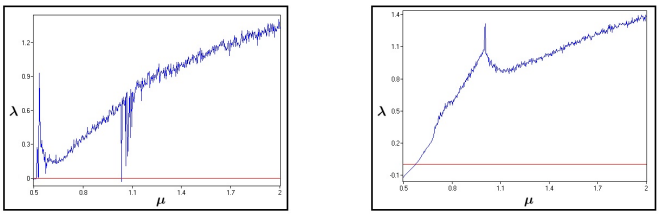
a) b)

Fig. 4. Bifurcation diagram of 2-D new maps a) TTL_μ^{RC} non-alternate (10) b) TTL_μ^{SC} alternate (11)

For both graphs starting from $\mu = 0$ to $\mu = 0.25$, we can observe a period 1 (*i.e.* a fixed point). Then the steady-state response undergoes a so-called pitchfork bifurcation to period 2. Following bifurcation undergoes multiple periods. At higher μ values, the behavior is generally chaotic. However, for TTL_μ^{RC} near $\mu = 1.1$ (Fig. 4.a) periodic windows appear. The subsequent intervals show perfect chaotic dynamics.

The Lyapunov exponent (LE) is a measure of the system sensitivity to initial conditions. The function of Lyapunov exponent λ is the characteristic of chaotic behavior in nonlinear maps. If $\lambda > 0$ the system exhibits chaotic behaviour.

Let us observe the graphics of Lyapunov exponent for TTL_μ^{RC} non-alternate (Fig. 5.a) and TTL_μ^{SC} alternate (Fig. 5.b) maps. For the plotting $10,000$ iterations were taken into account for every value of μ. The μ parameter is selected from 0.5 to 2. The list of points formed with μ is described on horizontal coordinate and the measure λ is on the vertical coordinate.



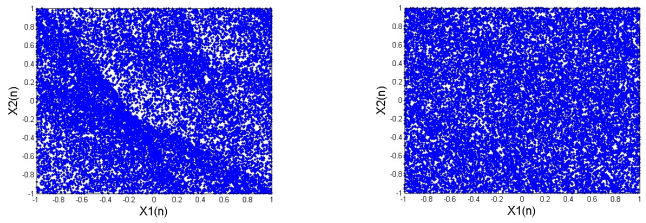
a) b)

Fig. 5. Function of the Lyapunov exponent for 2-D new maps a) TTL_μ^{RC} non-alternate map (10) b) TTL_μ^{SC} alternate map (11)

Graphs of the Lyapunov exponent are in exact agreement with bifurcations one. The measure λ is positive indicating chaotic dynamics which increases showing the strongest chaos at $\mu = 2$.

The study demonstrates that TTL_μ^{RC} non-alternate (Fig. 5.a) and TTL_μ^{SC} alternate (Fig. 5.b) maps exhibit the best chaotic behavior characteristics when $\mu = 2$, therefore we will continue our study fixing the parameter to this value. On the graphs for any given initial point x_0 trajectories will look like chaotic. Hence, we can study an attractor in phase space and phase delay.

Let us plot the attractor in the phase space: $x_n^{(1)}$ versus $x_n^{(2)}$ to analyse the points distribution. Observing graphs of chaotic attractor we can make decision about complexity, notice weakness or infer the randomness nature. To plot the attractor 3×10^4 points have been generated, 10^4 points of the transient regime have been cut off.



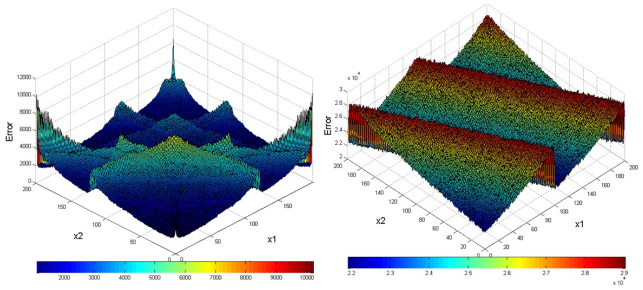
a) b)

Fig. 6. Phase space attractor of 2-D new maps, 2×10^4 points are generated a) TTL_2^{RC} non-alternate (10) b) TTL_2^{SC} alternate (11)

The graphs of the attractor in phase space for TTL_2^{RC} non-alternate (Fig. 6a) and TTL_2^{SC} alternate (Fig. 6b) maps are quite different. The first one has well scattered points on all the pattern, but there are some more "concentrated" regions forming curves on the graph.

The quality of the entire cryptosystem mostly depends on PRNG and one of the most important things for robust PRNG is uniform distribution of generated values in the space (Criterion 5, Fig. 3). An approximated invariant measure gives the best picture of probability. Thus, the invariant measure [15] is used for precise study of the points distribution. Using the approximate density function the best picture of points density can be achieved. The graph of the function demonstrates distribution comparison between regions. The size of each of the boxes is measured by $step$. In other words the plain

is divided $boxes[i,j]$ with square $step^2$, after the counts the number of points enter into the box $box[i,j]$ is counted.



a) b)

Fig. 7. Approximate density function, where $step = 0.01$, 10^9 points are generated a) TTL_2^{RC} non-alternate map b) TTL_2^{SC} alternate map

For the approximation function the pattern was divided into 200 boxes or $step = 0.01$, 10^9 points were generated. Note that those values are the maximal possible used to calculate with a laptop computers. The graphs (Figs. 7a and 7b of the detail points distribution demonstrates that both systems have not excellent distribution in phase space.

Good results are demonstrated with two different kinds of coupling, simple and ring-coupling in dimension 2, thus increasing the complexity of the system. However as those results are not completely satisfactory, an improved geometry of coupling is introduced allowing us to describe a new 2-D Chaotic Pseudo Random Number Generator (CPRNG). It was noticed that some parts of the graph are perfectly joined, giving us idea to improve points density using some correction in equations.

IV. Two new 2-D chaotic PRNG

Considering the results of section III it seems possible to improve the randomness of the 2-D topology. First, let us rewrite the mapping TTL_μ^{SC} alternate (11) where $\mu = 2$ as follows:

$$TTL_2^{SC}(x_n^{(1)}, x_n^{(2)}) = \begin{cases} x_{n+1}^{(1)} = 1 + 2(x_n^{(2)})^2 - 4|x_n^{(1)}| \\ x_{n+1}^{(2)} = 1 - 2(x_n^{(2)})^2 + 2(|x_n^{(1)}| - |x_n^{(2)}|) \end{cases} \tag{12}$$

The first problem is that top green coloured region occurs after injection is applied. Thus, we develop the system (15) in such a way that green coloured region "stays" in such position without injection mechanism. Secondly, we need to reduce the width of the region. Obviously, it is possible to achieve this need by reducing the impact of the state x^1, with the new following map:

$$MTTL_2^{SC}(x_n^{(1)}, x_n^{(2)}) = \begin{cases} x_{n+1}^{(1)} = 1 + 2(x_n^{(2)})^2 - 2|x_n^{(1)}| \\ x_{n+1}^{(2)} = 1 - 2(x_n^{(2)})^2 + 2(|x_n^{(1)}| - |x_n^{(2)}|) \end{cases} \tag{13}$$

with the injection mechanism (8) used as well, but restricted to 3 phases:

$$\begin{array}{c} if\ x_{n+1}^{(1)} > 1\ then\ substract\ 2 \\ if\ x_{n+1}^{(2)} < -1\ then\ add\ 2 \\ if\ x_{n+1}^{(2)} > 1\ then\ substract\ 2 \end{array} \tag{14}$$

The results of the modifications are demonstrated on Figs. 8, 7.a and 7.b. The injection mechanism in 3 phases (Fig. 8) matched regions in an excellent way. The techniques used, greatly improve the points density in the phase space (Figs. 7).

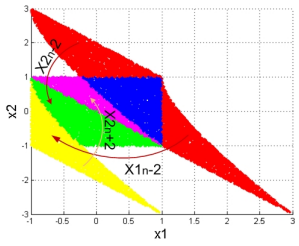
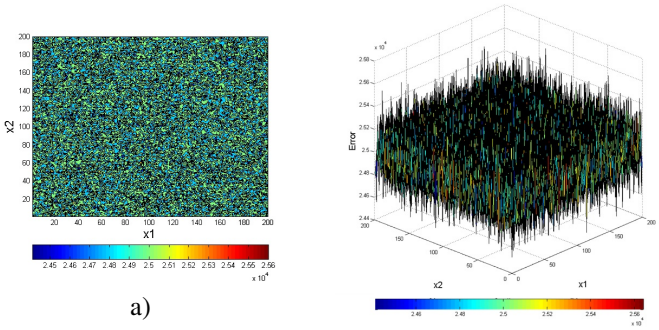


Fig. 8. Injection mechanism (14) of $MTTL_2^{SC}$ alternate map



a) b)

Fig. 9. Approximate density function of $MTTL_2^{SC}$ alternate map, where $step = 0.01$, 10^9 points are generated a) Boxes method b) 3D

The numerical results of the errors distributions (Fig. 10) shows excellent distribution till 10^9 points which is limited by the classical computer power. Moreover, the largest Lyapunov exponent is equal to 0.5905 indicating strong chaotic behavior.

The graph (Fig. 10) shows straight error reducing that proves, uniform points distribution when the number of iterates increases.

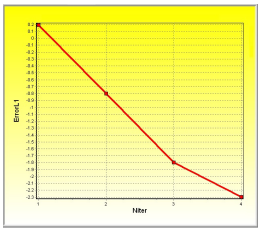
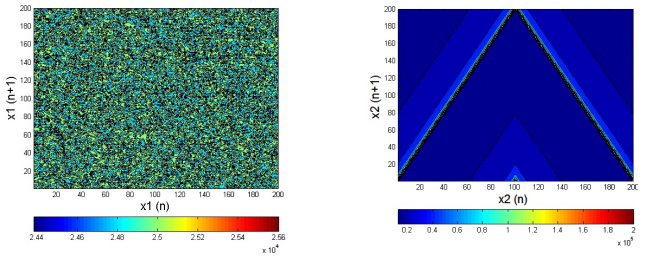


Fig. 10. Approximate distribution errors, for the system (13)

The points distribution of the attractor in phase delay is quite good as well (Fig. 11), where the plotting of 10^9 points are generated. In Fig. (11.b) tent distribution is recognized for $x^{(2)}$ variable but for encryption we need only output of one

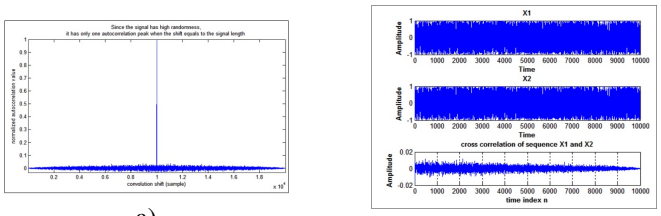
state (in our case $x^{(1)}$). Both states make strong impact on itself and for the global dynamics reaching significant points distribution on the torus and chaoticity.



a) b)

Fig. 11. a) Attractor in the phase delay, 10^9 points are generated, for the system (13) a) $(x_n^{(1)}, x_{n+1}^{(1)})$ b) $(x_n^{(2)}, x_{n+1}^{(2)})$

The $MTTL_2^{SC}$ alternate map is ring- and auto-coupled. Since one state takes part on creating dynamics of other one, both auto-correlation and cross-correlation have to be analysed for dependency and repeatability. The results of the 2-dimensional system are represented in Fig. 12. The same excellent results are in Fig. 12.a for autocorrelation, and in Fig. 12.b for cross-correlation, where the sequences on the graphs are near zero.



a) b)

Fig. 12. $MTTL_2^{SC}$ alternate map **a)** State autocorrelation analysis **b)** Correlation between states analysis

Topologically mixing means the system capability to progress over a short period of time. The system from any given initial region or open set of its phase space will ultimately be mixed up with any other region so that it is impossible to predict system evolution.

Here we represent graphical analysis of the 2-D $MTTL_2^{SC}$ alternate map for topological mixing. The square $[0,1]^2$ is divided into 4 quadrants and each of them are split into 15 boxes as well $(A2, B2, C2, \cdots, O2)$. 5×10^3 points have been generated in each of the boxes (Fig. 13). It is showed where the points from the initial boxes $(A1, B1, C1, \cdots, O1)$ of quadrant are mapped.

From the Fig. 13 it can be seen that points are distributed everywhere over the square, and it is hard to predict the next point or to find the previous one. The system is perfectly mixing because the regions are superimposed to each other. For example the blue colored region which is the image of the $A2$ box passes through the boxes $O1, I1, P1, C1, B1, E1, H1, M4, N4$ (Fig. 13). Colours and letters overlapping on the graphs vividly demonstrate that arbitrarily close points in some periods of time will have vastly different behaviors which means mixing.

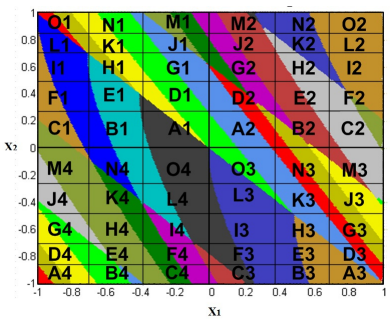


Fig. 13. Mixing boxes $(A \ldots O)$ and regions (coloured) in the phase space $(x_n^{(1)}, x_n^{(2)})$

NIST tests are used to verify randomness and system capability to resist main attacks when used for cryptographic purpose. They are used to prove PRNG robustness. NIST tests require only binary sequences, thus 4×10^6 points were generated, the first 5×10^5 were cut off. The rest of the sequence was converted to binary form according to the standard IEEE-754 (32 bit single precision floats).

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <data/Modified TL_{\mu}^{SC} alternative map_x1.txt>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
8	8	11	9	10	8	11	15	11	9	0.897763	100/100	Frequency
13	13	12	7	11	10	12	9	5	8	0.678686	99/100	BlockFrequency
6	7	5	12	16	12	12	9	14	7	0.191687	100/100	CumulativeSums
8	10	12	6	14	12	9	6	12	11	0.678686	100/100	Runs
14	11	12	10	15	7	6	13	8	6	0.236810	99/100	LongestRun
9	6	13	10	7	10	11	11	12	11	0.897763	97/100	Rank
11	12	6	19	4	11	11	13	8	5	0.037566	97/100	FFT
7	9	13	14	12	9	9	11	7	9	0.816537	100/100	NonOverlappingTemplate
10	11	15	10	11	9	12	6	11	5	0.595549	98/100	OverlappingTemplate
11	10	5	7	5	13	16	5	13	15	0.058984	100/100	Universal
14	6	11	10	7	9	13	12	8	10	0.739918	98/100	ApproximateEntropy
2	9	7	8	5	7	5	5	8	7	0.689019	63/63	RandomExcursions
5	8	4	4	6	4	4	11	6	11	0.222869	63/63	RandomExcursionsVariant
12	10	12	13	7	8	7	7	6	18	0.171867	99/100	Serial
9	13	11	12	7	9	7	16	7	9	0.534146	99/100	LinearComplexity

a)

Fig. 14. $MTTL_2^{SC}$ alternate map successfully passed NIST tests a) $x^{(1)}$

Both states of the generator successfully passed NIST tests (Fig. 14) demonstrating strong randomness and robustness against numerous statistical attacks.

We introduce now another structurally simple 2-D map using another topology. The map is described as follow:

$$NTTL_2^{SC}(x_n^{(1)}, x_n^{(2)}) = \begin{cases} x_{n+1}^{(1)} = 1 - 2|x_n^{(2)}| \\ x_{n+1}^{(2)} = 1 - 2(x_n^{(2)})^2 - 2(|x_n^{(2)}| - |x_n^{(1)}|) \end{cases} \quad (15)$$

applying injection mechanism (Fig. 15) to hold dynamics in $[-1,1]^2$:

$$\begin{array}{c} if\ x_{n+1}^{(2)} < -1\ then\ add\ 2 \\ if\ x_{n+1}^{(2)} > 1\ then\ substract\ 2 \end{array} \quad (16)$$

The $NTTL_2$ exhibits excellent density in phase delay for both states (Fig. 16), being very promising in real application.

The $NTTL_2$ map exhibits complex dynamics capable to refuse statistical attacks since it successfully passed NIST tests (Fig. 17).

The future work will be devoted to the investigation of topologies in 3 dimensional space where the complexity of

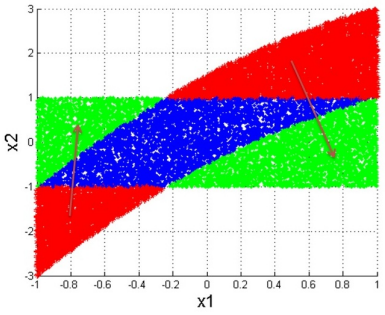
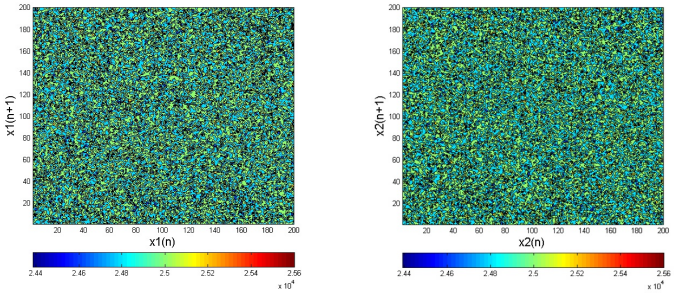


Fig. 15. Injection mechanism (14) of $NTTL_2$ alternate map



a) b)

Fig. 16. $NTTL_2$ density in phase delay **a)** $(x_n^{(1)}, x_{n+1}^{(1)})$ **b)** $(x_n^{(2)}, x_{n+1}^{(2)})$

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <data/x2.txt>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
5	12	10	5	12	12	15	7	14	8	0.236810	99/100	Frequency
8	9	14	8	6	12	12	10	10	11	0.834308	100/100	BlockFrequency
4	12	14	13	10	8	7	7	17	8	0.122325	100/100	CumulativeSums
10	9	10	15	9	12	9	8	9	9	0.924076	100/100	Runs
9	14	7	8	11	12	15	10	7	7	0.554420	100/100	LongestRun
10	11	11	4	14	13	8	13	11	5	0.334538	100/100	Rank
14	9	13	7	11	7	11	14	8	6	0.514124	99/100	FFT
6	10	10	11	5	18	12	3	9	16	0.020548	100/100	NonOverlappingTemplate
12	13	14	11	8	7	9	10	6	10	0.739918	100/100	OverlappingTemplate
7	12	13	16	11	13	13	5	5	5	0.085587	99/100	Universal
12	12	15	4	11	7	10	8	6	15	0.191687	100/100	ApproximateEntropy
3	9	7	7	10	7	6	3	6	6	0.568055	64/64	RandomExcursions
1	6	5	8	8	5	6	7	8	10	0.407091	64/64	RandomExcursionsVariant
14	8	11	10	11	14	9	2	9	12	0.289667	100/100	Serial
9	10	10	5	16	8	5	12	13	12	0.289667	100/100	LinearComplexity

a)

Fig. 17. $NTTL_2$ map successfully passed NIST tests

dynamical phenomena are expected to exhibit even better performances, though being more intricate [16]

V. Conclusion

In this paper we have proposed the original idea to couple two well-known chaotic maps (tent and logistic one), which considered separately - don't exhibit the required features for encryption purposes because they have weak security (collapsing effect) when applied alone. The new coupling changed qualitatively the overall system behavior, because the maps used with injection mechanism and coupling between states increased their complexity.

We have explored several topologies and finally proposed two new 2-D CPRNG. The proposed models with injection mechanism allow to puzzle perfectly the pieces of the chaotic attractor, like a true random generator. To achieve the best distribution in the phase space, the modified form $MTTL_2^{SC}$ alternate map has been proposed. The new map exhibits excellent features due to the injection mechanism and enables the uniform density in the state space. The system exhibits strong nonlinear dynamics, demonstrating great sensitivity to initial conditions. It generates an infinite range of intensive chaotic behavior with large positive Lyapunov exponent values. Moreover, $MTTL_2^{SC}$ successfully passed all required tests: cross-correlation, autocorrelation, LLE, NIST tests, uniform attractor on the phase space and phase delay. The system analysis and the dynamics evolution by bifurcation diagram and topological mixing proved the complex behavior. The system orbits exhibited complex behavior with perfect mixing. The study demonstrated totally unpredictable (for any intruder) dynamics making the system strong-potential candidate for high-security applications. Another CPRNG candidate based on $NTTL_2^{SC}$ map was proposed that successfully passed all required statistical, graphical and numerical results for both states components. The $NTTL_2^{SC}$ map demonstrates complex dynamics being very promising to real scale cryptography application.

References

[1] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. CRC press, 1996.

[2] C.-Y. Li, Y.-H. Chen, T.-Y. Chang, L.-Y. Deng, and K. To, "Period extension and randomness enhancement using high-throughput reseeding-mixing prng," *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, vol. 20, no. 2, pp. 385–389, 2012.

[3] R. M. May, *Stability and complexity in model ecosystems*. Princeton University Press, 2001, vol. 6.

[4] R. M. May *et al.*, "Biological populations with nonoverlapping generations: stable points, stable cycles, and chaos," *Science*, vol. 186, no. 4164, pp. 645–647, 1974.

[5] M. J. Feigenbaum, "The universal metric properties of nonlinear transformations," *Journal of Statistical Physics*, vol. 21, no. 6, pp. 669–706, 1979.

[6] B. Sudret, "Global sensitivity analysis using polynomial chaos expansions," *Reliability Engineering & System Safety*, vol. 93, no. 7, pp. 964–979, 2008.

[7] R. Lozi, "Can we trust in numerical computations of chaotic solutions of dynamical systems?" *In Topology and Dynamics of Chaos, Ch. Letellier, R. Gilmore (Eds.), World Scientific Series in Nonlinear Science Series A , Chapt. 3*, 2013.

[8] M. Ariffin and M. Noorani, "Modified baptista type chaotic cryptosystem via matrix secret key," *Physics Letters A*, vol. 372, no. 33, pp. 5427–5430, 2008.

[9] R. Lozi, "Designing chaotic mathematical circuits for solving practical problems," *International Journal of Automation and Computing*, vol. 11, no. 6, pp. 588–597, 2014.

[10] G. Yuan and J. A. Yorke, "Collapsing of chaos in one dimensional maps," *Physica D: Nonlinear Phenomena*, vol. 136, no. 1, pp. 18–30, 2000.

[11] O. E. Lanford III, "Informal remarks on the orbit structure of discrete approximations to chaotic maps," *Experimental Mathematics*, vol. 7, no. 4, pp. 317–324, 1998.

[12] W.-K. Wong, L.-P. Lee, and K.-W. Wong, "A modified chaotic cryptographic method," in *Communications and Multimedia Security Issues of the New Century*. Springer, 2001, pp. 123–126.

[13] H. Nejati, A. Beirami, and Y. Massoud, "A realizable modified tent map for true random number generation," in *Circuits and Systems, 2008. MWSCAS 2008. 51st Midwest Symposium on*. IEEE, 2008, pp. 621–624.

[14] A. E. Rojas, I. Taralova, R. Lozi *et al.*, "New alternate ring-coupled map for multi-random number generation," *Journal of Nonlinear Systems and Applications*, vol. 4, no. 1, pp. 64–69, 2013.

[15] R. Lozi, "Chaotic pseudo random number generators via ultra weak coupling of chaotic maps and double threshold sampling sequences," *In proceedings of: ICCSA 2009 The 3rd International Conference on Complex Systems and Applications, University of Le Havre, France, June 29-July 02 (2009)*, pp. 20–24, 2009.

[16] G. Manjunath, D. Fournier-Prunaret, and A.-K. Taha, "A 3-dimensional piecewise affine map used as a chaotic generator," *European Conference on Iteration Theory September(ECIT), Yalta, Ukraine*, pp. 7–13, 2008.